



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/596,745	06/19/2000	Carl J. Kraenzel	LOT9 2000 0011 US1	3997

7590 02/12/2004
Stephen T. Keohane, Esq.
Lotus Development Corporation
55 Cambridge Parkway
Cambridge, MA 02142

EXAMINER

CHOUDHARY, ANITA

ART UNIT	PAPER NUMBER
----------	--------------

2153

DATE MAILED: 02/12/2004

13

Please find below and/or attached an Office communication concerning this application or proceeding.

22

Office Action Summary

Application No.

09/596,745

Applicant(s)

KRAENZEL ET AL.

Examiner

Anita Choudhary

Art Unit

2153

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 May 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

The amendment filed on 11/26/2003 under 37 CFR 1.312 has been entered. Claims 1, 7, 12, 17, 18, and 19 have been amended and are presented for further examination.

Claims 1-19 are presented.

Response to Arguments

Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerger et al (US 6,473,800) in view of Moriconi et al. (US 6,158,010).

Jerger shows a computer system for providing security when downloading foreign content from a computer network server. Foreign content is untrusted code that may attempt to run on the client machine. Before code is downloaded to client machine in a respective zone, specific security actions are taken depending on various settings of each respective zone (see col.

Art Unit: 2153

3 lines 5-27). Security zones administer different privileges and different levels of trust are established for each corresponding zone consisting of a group of network locations (see col. 8 lines 1-4). More specifically, in referring to claim 1, Jerger shows:

- A connection protocol connecting a user client to a server site (column 1, lines 41-44);
- Download utilities responsive to said connection protocol for downloading said services and programs from said server site to said user client (column 3, lines 15-16); and
- Trust assignment user interface dialogs responsive to said connection protocol for advising said user of risks taken when accepting executable download from said server site (see Fig. 5B and column 2, lines 27-31 and 36-38 and column 19, lines 66-67 and column 20, lines 1-6).

Although Jerger shows substantial features of the claimed invention, Jerger does not explicitly show downloading to *separate and non-conflicting execution spaces at said user client; nor said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs*. Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Moriconi.

In an analogous art, Moriconi show a system for secure distribution of application components and objects to client using distribution security policy located at server. Essentially Moriconi shows a central server for controlling security operations of application running on clients. Moriconi shows a group of clients being assigned a “role”. Roles are named groups of privileges that are granted to members of that role (see col. 7 lines 41-58). Moriconi shows:

Art Unit: 2153

Download utilities for downloading services and programs from server site to separate and non-conflicting execution spaces at said users client (col. 8 lines 7-14, col. 10 lines 27-32).

Server site responsive to said user accepting server site as trusted for centrally administering security policies for said services and programs executing at said user client (col. 9 lines 24-44).

Given these features, a person of ordinary skill in the art would have readily recognized the desirability and advantages of modifying the system shown by Jerger to employing the well known features shown by Moriconi, in order to more securely administer the distribution of sensitive application information from a secure server site to a client (see Moriconi col. 3 lines 32-48).

In considering **claim 2**, Jerger discloses said connection protocol selectively being HTTP or HTTPS (see Fig. 4B, “433” and column 18, lines 8-10 and column 17, lines 61-66).

In considering **claim 3**, Jerger discloses the system further comprising:

a processor for establishing security context (see column 14, lines 52-54), said processor including

a stage 1 processor for determining from said user if said server site is to be trusted (see column 14, lines 54-57 and 64-67); and

a stage 2 processor for establishing whether or not the identity of said web site is confirmed and determining from said user if processing should continue to include installation of programs on said client (see column 20, lines 2-11).

In considering **claim 4**, Jerger discloses the system further comprising:

a client download page (see column 3, lines 29-32);

a download control element in said download page (see column 3, lines 29-32);

Art Unit: 2153

said processor being activated upon activation of said download control element within said download page initiating a download process first to establish a security context and then to download program executable files (see column 3, lines 32-37).

In considering **claim 5**, Jerger discloses the system further comprising:

said download utilities being responsive to an SSL connection to said server for activating said dialog to advise said user that said server site has been verified as being what it represents itself to be and to query said user whether code is to be downloaded from said server site to said client (see column 18, lines 13-16 and Fig. 4B, "433" and column 20, lines 2-11).

In considering **claim 6**, Jerger discloses said code being custom code (see Fig. 5B).

In considering **claim 7**, Jerger discloses said download utilities being responsive to a connection from said client to said server being other than SSL for activating said dialog to advise said user that said server site has not been verified as being what it represents itself to be and to query said user whether code is to be downloaded from said server site to said client (see column 22, lines 13-14 and lines 59-60).

In considering **claim 8**, Jerger discloses said code being custom code (see Fig. 5B).

In considering **claim 9**, Jerger discloses the system further comprising:

said download utilities being responsive to user acceptance of download from said server site of executable code for downloading said executable code to said client (see column 18, lines 27-28 and Fig. 5B); and

a trace utility for identifying originators of downloaded code (see column 22, lines 9-13).

In considering **claim 10**, Jerger discloses said trace utility selectively identifying originators of signed agents through electronic signature, of custom code traceable to code

Art Unit: 2153

vendor through web site relationship, or custom code directly created by said web site (see column 22, lines 9-13).

In considering **claim 11**, Jerger discloses the system further comprising:

a first trust model for establishing level of traceable accountability for a subscription at download time over a secure connection protocol (see column 23, lines 33-37 and 47-50);

a second trust model for establishing a reduced level of traceable accountability, with traceable accountability established only for electronically signed agents used by said subscription over a connection protocol not verified as secure (see column 24, lines 35-42); and said dialogs being responsive to said trust models (see Fig. 5B, "510").

In considering **claim 12**, Jerger discloses a method for governing delivery of services and programs from a workflow, enterprise and mail enabled application server and platform according to a web based trust model, comprising the steps of:

- Establishing a connection protocol between a client and a web site (see column 1, lines 41-44);
- Responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from said web site (see column 14, lines 49-52 and column 16, lines 41-50);
- Advising a user at said client of said trust level assignable with respect to said risks to said web site (see column 2, lines 27-31 and 36-38 and Fig. 5B); and
- Responsive to user acceptance of said risks and accepting said server site as trusted, downloading said services and programs from a server site to said user client (see column 20,

Art Unit: 2153

lines 5-6; Note that if the user selects “yes” the operation, i.e. downloading services and programs, is to be performed.).

Although Jerger shows substantial features of the claimed invention, Jerger does not explicitly show downloading to *separate and non-conflicting execution spaces at said user client*; nor *said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs*. Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Moriconi.

In an analogous art, Moriconi show a system for secure distribution of application components and objects to client using distribution security policy located at server. Essentially Moriconi shows a central server for controlling security operations of application running on clients. Moriconi shows a group of clients being assigned a “role”. Roles are named groups of privileges that are granted to members of that role (see col. 7 lines 41-58). Moriconi shows:

Download utilities for downloading services and programs from server site to separate and non-conflicting execution spaces at said users client (col. 8 lines 7-14, col. 10 lines 27-32).

Server site responsive to said user accepting server site as trusted for centrally administering security policies for said services and programs executing at said user client (col. 9 lines 24-44).

Given these features, a person of ordinary skill in the art would have readily recognized the desirability and advantages of modifying the system shown by Jerger to employing the well known features shown by Moriconi, in order to more securely administer the distribution of sensitive application information from a secure server site to a client (see Moriconi col. 3 lines 32-48).

In considering **claim 13**, Jerger discloses the method further comprising the steps of:
displaying a download control element in a client download page (see column 3, lines 29-32);

responsive to user selection of said download control element or upon schedule, initiating a download process first to establish a security context and then to download program executable files from said server (see column 3, lines 32-37).

In considering **claim 14**, Jerger discloses the method further comprising the step of responsive to user acceptance of download from said server site of executable code, downloading said executable code to said client (see column 18, lines 27-28 and Fig. 5B).

In considering **claim 15**, Jerger discloses the method further comprising the step of identifying originators of downloaded code (see column 22, lines 9-13).

In considering **claim 16**, Jerger discloses the method further comprising the step of selectively identifying originators of signed agents through electronic signature, of custom code traceable to code vendor through web site relationship, or custom code directly created by said web site (see column 22, lines 9-13).

- In considering **claim 17**, Jerger discloses the method further comprising the steps of:
- Establishing a first trust model specifying a level of traceable accountability for a subscription at download time over a secure connection protocol (see column 23, lines 33-37 and 47-50);
 - Establishing a second trust model for specifying a reduced level of traceable accountability, with traceable accountability established only for electronically signed agents used by said

Art Unit: 2153

subscription over a connection protocol not verified as secure (see column 24, lines 35-42);
and

- Said dialogs being responsive to said trust models (see Fig. 5B, “510”).

In considering **claim 18**, Jerger discloses a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for governing delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform according to a web based trust model, said method steps comprising:

- Establishing a connection protocol between a client and a web site (see column 1, lines 41-44);
- Responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from said web site (see column 14, lines 49-52 and column 16, lines 41-50);
- Advising a user at said client of said trust level assignable with respect to said risks to said web site (see column 2, lines 27-31 and 36-68 and Fig. 5B); and
- Responsive to user acceptance of said risks and I accepting said server site as trusted, downloading said services and programs from a server site to said user client (see column 20, lines 5-6; Note that if the user selects “yes” the operation, i.e. downloading services and programs, is to be performed.).

Although Jerger shows substantial features of the claimed invention, Jerger does not explicitly show downloading to *separate and non-conflicting execution spaces* at said user client; nor *said server site responsive to said user accepting said server site as trusted for centrally*

Art Unit: 2153

administering security policies for said services and programs for centrally determining and controlling services and programs to be executed at said client. Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Moriconi.

In an analogous art, Moriconi show a system for secure distribution of application components and objects to client using distribution security policy located at server. Essentially Moriconi shows a central server for controlling security operations of application running on clients. Moriconi shows a group of clients being assigned a "role". Roles are named groups of privileges that are granted to members of that role (see col. 7 lines 41-58). Moriconi shows:

Server site responsive to said user accepting server site as trusted, downloading services and programs from server site to separate and non-conflicting execution spaces at said users client (col. 8 lines 7-14, col. 10 lines 27-32) and centrally administering security policies for said services and programs for centrally determining and controlling services and programs to be executed at said client (col. 9 lines 10-44).

Given these features, a person of ordinary skill in the art would have readily recognized the desirability and advantages of modifying the system shown by Jerger to employing the well known features shown by Moriconi, in order to more securely administer the distribution of sensitive application information from a secure server site to a client (see Moriconi col. 3 lines 32-48).

In considering **claim 19**, Jerger discloses a computer program product configured to be operable to govern delivery of services and programs from a workflow, enterprise and mail-

Art Unit: 2153

enabled application server and platform according to a web based trust model, according to the steps of:

- Establishing a connection protocol between a client and a web site (see column 1, lines 41-44);
- Responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from said web site (see column 14, lines 49-52 and column 16, lines 41-50);
- Advising a user at said client of said trust level assignable with respect to said risks to said web site (see column 2, lines 27-31 and 36-38 and Fig. 5B); and
- Responsive to user acceptance of said risks and accepting said server site as trusted, downloading said services and programs from a server site to said user client (see column 20, lines 5-6; Note that if the user selects “yes” the operation, i.e. downloading services and programs, is to be performed.).

Although Jerger shows substantial features of the claimed invention, Jerger does not explicitly show downloading to *separate and non-conflicting execution spaces* at said user client; nor *said server site responsive to said user accepting said server site as trusted for centrally administering from said server site security policies for control which said services and programs shall be executed at said client*. Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Moriconi.

In an analogous art, Moriconi show a system for secure distribution of application components and objects to client using distribution security policy located at server. Essentially

Art Unit: 2153

Moriconi shows a central server for controlling security operations of application running on clients. Moriconi shows a group of clients being assigned a "role". Roles are named groups of privileges that are granted to members of that role (see col. 7 lines 41-58). Moriconi shows:

Server site responsive to said user accepting server site as trusted, downloading services and programs from server site to separate and non-conflicting execution spaces at said users client (col. 8 lines 7-14, col. 10 lines 27-32) and centrally administering from said server site security policies for control which said services and programs shall be executed at said client (col. 9 lines 10-44).

Given these features, a person of ordinary skill in the art would have readily recognized the desirability and advantages of modifying the system shown by Jerger to employing the well known features shown by Moriconi, in order to more securely administer the distribution of sensitive application information from a secure server site to a client (see Moriconi col. 3 lines 32-48).

Conclusion

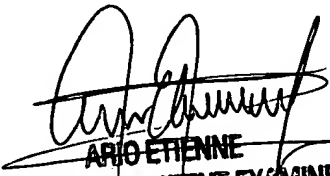
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anita Choudhary whose telephone number is (703) 305-5268. The examiner can normally be reached on 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached on (703) 305-4792. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2153

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AC
February 3, 2004


ARIO ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100